Mashable

4 Legal Considerations for Building a Mobile App

Alysa Z. Hutnik is a partner in the Advertising Law and Privacy & Information Security practices at Kelley Drye & Warren LLP. Her co-author, Christopher M. Loeffler, is an advertising and privacy associate at Kelley Drye & Warren LLP. Read more on Kelley Drye's advertising blog Ad Law Access or keep up with the group on Facebook or Twitter.

If creating a mobile app is next on your business agenda, you're not alone. A recent report pegs mobile app revenue from the four major application stores at $2.1 billion in 2010. Revenue is forecast to grow a staggering 77.7% in 2011 to $3.8 billion, and smartphone adoption rates continue to increase.

Whether your app is destined for an *Angry Birds*-like following or will serve a more niche market, your development checklist should address traditional legal items for a new business venture. Given the broad consumer audience that comes with many mobile apps, it's helpful to keep in mind the types of issues tracked closely by the consumer protection bar, consumer advocates, regulators and private litigants.

Their scrutiny essentially boils down to two core questions:

- Are there any unexpected (bad) surprises connected with your app from a user experience — namely, does the app clearly convey all potential monetary charges (both initial download and in-app options)?
- What information from the user and the device will be collected and shared with others, and was that clearly disclosed and consented to before data was collected/shared?

Failure to identify and address these issues can result in complaints and negative media coverage and quickly turn positive app buzz into formal inquiries and lawsuits. *The Wall Street Journal*'s ongoing "What They Know" series, among other media exposés, has helped generate some of this unwanted attention for a number of parties in the mobile device, app and marketing sectors, including Apple, Google and Pandora.

While it will take years for regulators and case law to solidify the legal boundaries around any emerging technology, including mobile apps, businesses and marketers who want to avoid predictable legal scrutiny can reduce their risks now by adhering to traditional best practices around advertising and privacy.

This article originally appeared on Mashable.com.
Published: May 26, 2011

Mashable

Start With This Checklist

Don't Hide the Money Factor. If your app has a charge associated with it — whether as part of the initial purchase or within the app itself (e.g. purchase in-game content, accessories, etc.), disclose that point upfront using plain language in the description. Apply a "dummy" test — would your tech-challenged family member notice and read the disclosure, or is it buried under miles of terms and conditions?

Definitely Don't Hide the Money Factor if Your App is Targeted at Kids. If you expect that parents will be downloading your free app but kids will be playing it, consider whether in-game charges make sense from a business standpoint (weighed against the risks of parents claiming unauthorized charges by their children). If there is a sound business reason for the in-game charge options, make sure you clearly and conspicuously disclose the potential for charges up front in the description.

Assess Your Data Drilling. Unless you're closely watching courts and Congress, you might not have realized that mobile app user data comes with strings attached. You must assess exactly what user data your app is collecting (intentionally and unintentionally) and why it is doing so. Ask yourself these questions:

- Does this data collection involve name, contact details or other personally identifiable information on the user or their contacts?
- Does the app collect device location information and/or a unique identifier per user or device?
- Is there a necessary business reason for that data collection and access?
- Do you retain that data for a period of time consistent with the reason for collecting it?
- Do you share that data with other parties (or allow others to access that data), and can the parties use the data to make a personally identifiable profile of your users?

If you answered "yes" to any of the above, you should closely review how/if your app's terms communicate that to the user and whether users understand those terms and provide consent for such use.

Legalese Is Bad. If you plan to take care of everything identified above with a link to a lengthy boilerplate terms and conditions and privacy policy, think again. A legalese boilerplate won't insulate your business. The overriding question is whether you clearly communicated important terms — like charges and personal data practices — to the consumer in a way the consumer understood and accepted. That means ensuring that your app walks the user through these key terms in a just-in-time, user-friendly way.

This article originally appeared on Mashable.com.
Published: May 26, 2011